Utilizando NAT em redes sobrepostas

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento demonstra como você pode usar a Conversão de endereço de rede (NAT) para sobrepor redes. As redes sobrepostas resultam quando você atribui um endereço IP a um dispositivo em sua rede que já está legalmente ocupado e atribuído a um dispositivo diferente na Internet ou rede externa. As redes sobreposta igualmente resultarem quando duas empresas, ambos de quem endereços IP do RFC 1918 do uso em suas redes, fusão. Essas duas redes precisam se comunicar, de preferência sem ter que endereçar novamente todos os seus dispositivos.

Prerequisites

Requirements

Uma compreensão básica do endereçamento IP, do roteamento IP e do DNS (Domain Name System) é útil para entender o conteúdo deste documento.

Componentes Utilizados

O suporte para NAT começou na versão 11.2 do software Cisco IOS®. Para obter mais informações sobre suporte da plataforma, consulte Perguntas frequentes sobre NAT.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

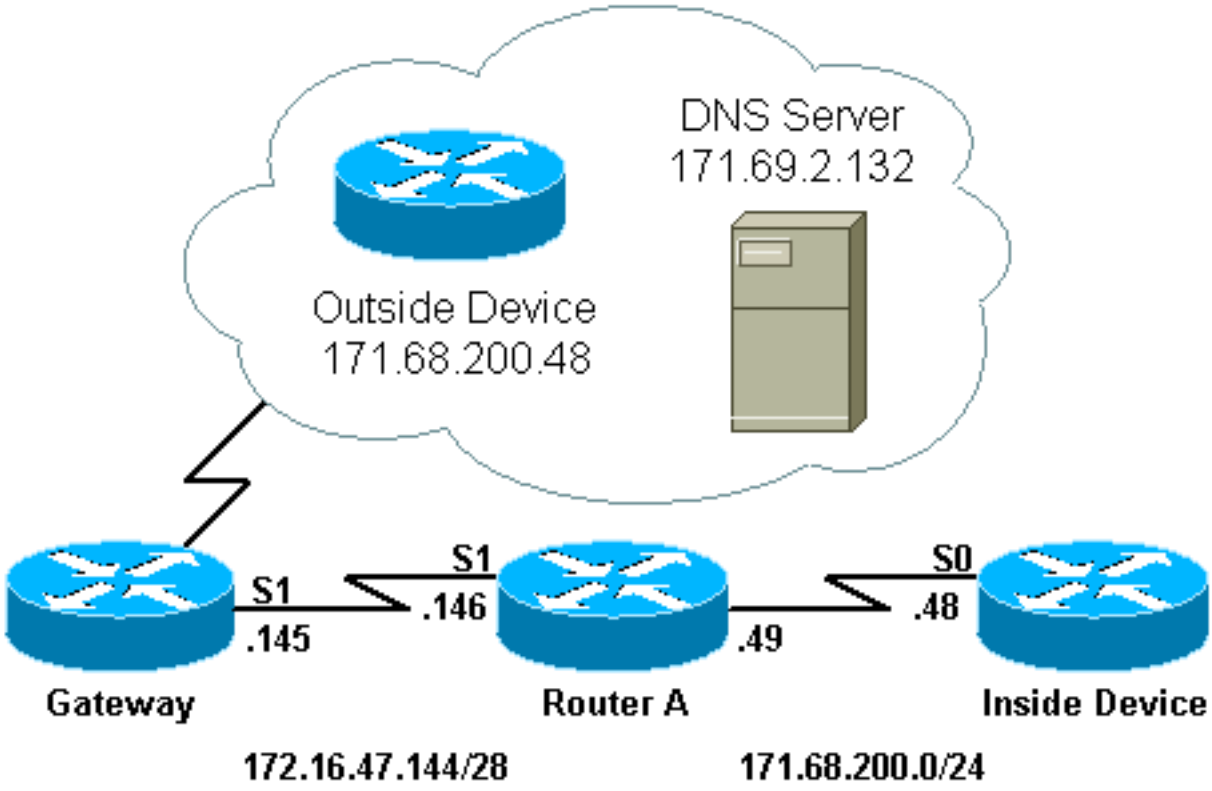
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

Observe que o dispositivo interno tem o mesmo endereço IP que o dispositivo externo com o qual deseja se comunicar.



Configurações

O Roteador A é configurado para NAT, de modo que converta o dispositivo interno em um endereço do pool "test-loop" e do dispositivo externo em um endereço do pool "test-dns". Uma explicação de como essa configuração ajuda na sobreposição segue a tabela de configuração abaixo.

Router A
`` ! version 11.2 no service udp-small-servers no service tcp-small-servers ! hostname Router-A ```

```
!
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Para que a configuração acima ajude com a sobreposição quando o dispositivo interno se comunica com o dispositivo externo, ele deve usar o nome de domínio do dispositivo externo.

O dispositivo interno não pode usar o endereço IP do dispositivo externo porque é o mesmo endereço atribuído a si mesmo (o dispositivo interno). Portanto, o dispositivo interno enviará uma consulta DNS para o nome de domínio do dispositivo externo. O endereço IP do dispositivo interno será a origem dessa consulta e esse endereço será convertido para um endereço do pool de "test-loop" porque o comando **ip nat inside source list** está configurado.

O servidor DNS responde ao endereço que veio do pool "test-loop" com o endereço IP associado ao nome de domínio do dispositivo externo no payload do pacote. O endereço destino do pacote de resposta é convertido de volta ao endereço do dispositivo interno, e o endereço no payload do pacote de resposta é convertido em um endereço do pool "test-dns" devido ao comando **ip nat outside source list**. Portanto, o dispositivo interno aprende que o endereço IP do dispositivo externo é um dos endereços do pool "test-dns" e usará esse endereço ao se comunicar com o

dispositivo externo. O roteador que executa o NAT cuida das conversões neste ponto.

Esse processo pode ser visto em detalhes na seção Solução de problemas. Os dispositivos que usam endereços sobrepostos podem se comunicar entre si sem o uso de DNS, mas nesse caso, o NAT estático teria que ser configurado. Segue-se um exemplo de como isso pode ser feito.

Router A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
!--- This line is necessary to make NAT work for return
traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. access-list 7 permit 171.68.200.0
0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Com a configuração acima, quando o dispositivo interno deseja se comunicar com o dispositivo externo, ele agora pode usar o endereço IP 172.16.47.177, e o DNS não é necessário. Como mostrado acima, a conversão do endereço do dispositivo interno ainda é feita dinamicamente, o que significa que o roteador deve obter pacotes do dispositivo interno antes que uma conversão seja criada. Por esse motivo, o dispositivo interno deve iniciar todas as conexões para que o dispositivo interno e o dispositivo externo se comuniquem. Se for necessário que o dispositivo externo inicie conexões com o dispositivo interno, o endereço do dispositivo interno também deve ser configurado estaticamente.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O processo pelo qual o dispositivo interno usou o DNS para se comunicar com o dispositivo externo, conforme descrito acima, pode ser visualizado em detalhes com o seguinte processo de solução de problemas.

Atualmente, não há conversões na tabela de conversões que possam ser vistas com o comando show ip nat translations. Os exemplos abaixo usam os comandos **debug ip packet** e **debug ip nat**.

Observação: os comandos **debug** geram uma quantidade significativa de saída. Use-o somente quando o tráfego na rede IP for baixo, para que outra atividade no sistema não seja afetada de forma prejudicial.

```
Router-A# show ip nat translations
Router-A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
```

Quando o dispositivo interno envia sua consulta DNS para o servidor DNS, que reside fora do domínio NAT, o endereço de origem da consulta DNS (o endereço do dispositivo interno) é convertido devido aos comandos ip nat inside. Isso pode ser visto na saída de depuração abaixo.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=6988, dst=53
```

Quando o servidor DNS envia uma resposta DNS, o payload da resposta DNS é traduzido, devido aos comandos ip nat outside.

Observação: o NAT não examina o payload da resposta DNS, a menos que a conversão ocorra no cabeçalho IP do pacote de resposta. Consulte o comando ip nat outside source list 7 pool na configuração do roteador a seguir.

A primeira mensagem de NAT na saída de depuração abaixo mostra que o roteador reconhece a

resposta DNS e converte o endereço IP dentro do payload para 172.16.47.177. A segunda mensagem de NAT mostra o roteador convertendo o destino da resposta de DNS para poder encaminhar uma resposta de retorno para o dispositivo de entrada que executou a consulta de DNS inicial. A parte de destino do cabeçalho, o endereço global interno, é convertida para o endereço local interno.

O payload da resposta do DNS foi traduzido.

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

A porção de destino do cabeçalho de IP no pacote de resposta DNS é traduzida:

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```

Vejamos outra consulta e resposta DNS:

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

Agora que o payload do DNS foi convertido, a tabela de conversão tem uma entrada para os endereços externos local e global do dispositivo externo. Com essas entradas na tabela, podemos traduzir completamente o cabeçalho dos pacotes ICMP trocados entre o dispositivo interno e o dispositivo externo. Vamos observar essa intercâmbio na saída de depuração a seguir.

A seguinte saída mostra o endereço de origem (endereço do dispositivo interno) que está sendo traduzido.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```

Aqui, o endereço de destino (endereço local externo do dispositivo externo) é convertido.

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```

Após a tradução, o pacote IP tem a seguinte aparência:

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

A seguinte saída mostra o endereço de origem (endereço do dispositivo de saída) que está sendo traduzido no pacote de informação de retorno.

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```

Agora o endereço de destino (dentro do endereço global do dispositivo) do pacote de retorno é traduzido.

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```

Após a tradução, o pacote de retorno se parece com isto:

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

A troca de pacotes entre o dispositivo interno e o dispositivo externo continua.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Após a conclusão da troca de pacotes entre a parte externa e interna, podemos observar a tabela de conversões, que possui três entradas. A primeira entrada foi criada quando o dispositivo interno enviou uma consulta DNS. A segunda entrada foi criada quando o payload da resposta de DNS foi convertido. A terceira entrada foi criada quando o ping foi trocado entre o dispositivo interno e o dispositivo externo. A terceira entrada é um resumo das duas primeiras entradas e é usada para conversões mais eficientes.

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
--- ---                ---                172.16.47.177      171.68.200.48
--- 172.16.47.161      171.68.200.48      172.16.47.177      171.68.200.48
```

Éimportante observar que ao tentar estabelecer a conectividade entre duas redes sobrepostas executando NAT dinâmico em um único roteador Cisco, você deve usar DNS para criar uma tradução global externa local para externa. Se você não usa DNS, a conectividade pode ser estabelecida com NAT estático, mas é mais difícil de gerenciar.

Informações Relacionadas

- Página de suporte de NAT
- Suporte Técnico - Cisco Systems